Quantum algorithm for finding collisions of hash functions

12 ランダムハッシュ関数の衝突を発見する量子アルゴリズム

量子技術による強い攻撃でもその暗号安全ですか

どんな研究	近年、量子計算機の研究開発の進展を背景に、量子計算機を用いた強力な攻撃を考慮に入れた、暗号の安全性評価が必要になってきています。この安全性評価のためには、具体的な攻撃手法が必要です。本展示では、暗号の中核技術であるハッシュ関数に対する、量子計算機を用いた攻撃手法をご紹介します。
どこが凄い	暗号の中核技術であるハッシュ関数に対して、量子計算機を用いた最高速の攻撃手法を発見しました。本手法の攻撃速度は理論限界を達成しており、理論上可能な最強の攻撃手法と言えます。また、汎用的な手法であるため、様々なハッシュ関数の安全性評価に利用可能です。
めざす未来	ハッシュ関数は、日常生活で使われている電子署名やユーザ認証に加え、最近では、ブロックチェーンなどにも利用される、中核的な暗号技術です。本成果は、現在進んでいる耐量子計算機暗号の議論における、ハッシュ関数の安全性解析に重要な知見を与えることにより、将来においても安全な暗号の開発に貢献します。

背景と成果の概要

- **暗号技術の安全性は、攻撃にかかる時間の膨大さで評価**
  例）「現在最高速の計算機でも解読に数百億年必要」
- 量子計算機の研究開発の進展を背景に、**量子計算機を用いた強力な攻撃を考慮に入れた、安全性**(攻撃に必要な時間)**の評価が必要**に

暗号の中核技術である**ハッシュ関数**に関して、**多重衝突**を発見(＝攻撃)するための、**量子計算機を用いた最高速アルゴリズムを発見**
➪様々なハッシュ関数の安全性評価に利用可能

ハッシュ関数

入力の推測が難しい短いデータを出力

入力 d: Quantum information science is expected to be an important field in information processing in the near future.

ハッシュ関数 f

出力 $f(d)$: rbxXx....zp7kMY

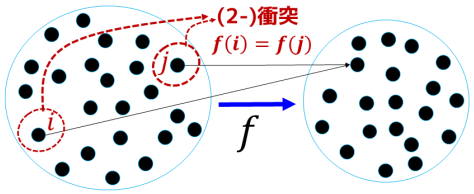
利用

改ざん防止等が必要な、非常に多くの場面で利用

電子署名 ➡Web暗号化 TLS/SSL / ユーザ認証 / 公開鍵暗号（RSA） / ブロックチェーン・暗号資産

ハッシュ関数の衝突

要素のペア(i,j) が関数fにより同じ値に移されるとき($f(i)=f(j)$)、ペア(i,j) を(2-)衝突と言う。同様に、fにより同じ値に移されるℓ個の要素をℓ-衝突と言う。(例えば、3-衝突の場合、$f(i)=f(j)=f(k)$)



衝突が発見できると、文書の改ざんなどができてしまう（例：同じ電子署名を持つ異なる文書に差し替える）
➪衝突発見の困難性(=膨大な時間を要するかどうか)を評価する必要
➪この評価のためには，**衝突を発見するアルゴリズムが必要**

ハッシュ関数の安全性向上の原動力＝衝突発見アルゴリズムの考案
標準的に利用されているハッシュ関数の世代交代は、
安全性を脅かす「衝突発見アルゴリズム」の考案により起こってきた

MD5 ['91] ➡ SHA-1 ['95] ➡ SHA-2 ['02] ➡ SHA-3 ['15]

アルゴリズムの詳細

以下では，ハッシュ関数のℓ-衝突発見問題に対する量子アルゴリズムの「理論的に保証された性能」と「動作の概略」を説明する

一様ランダムに選ばれたハッシュ関数*
$f:\{1,\cdots,M\}\to\{1,\cdots,N\}\ \ (\mathrm{M}\geq N)$

に対するℓ-衝突発見問題を解く量子アルゴリズムを構築し、
$N^{\frac{1}{2}\left(1-\frac{1}{2^{\ell}-1}\right)}$**時間***で 動作することを証明。 *$f$の計算は十分高速であると仮定

◎理論的に可能な速度上限を達成([LZ20]による下界と一致)

既存アルゴリズム[HSX17]との計算速度比較

各多重度(ℓ)に対して、ハッシュ値の総数(N)と多重衝突を発見するために要する時間の関係を表す

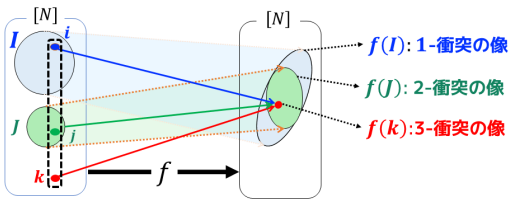
ℓ (多重度)	2	3	4	5	・・・	ℓ
既存結果[HSX17]	$N^{\frac{1}{3}}$	$N^{\frac{4}{9}}$	$N^{\frac{13}{27}}$	$N^{\frac{40}{81}}$	・・・	$N^{\frac{1}{2}\left(1-\frac{1}{3^{\ell}-1}\right)}$
提案アルゴリズム	$N^{\frac{1}{3}}$	$N^{\frac{3}{7}}$	$N^{\frac{7}{15}}$	$N^{\frac{15}{31}}$	・・・	$N^{\frac{1}{2}\left(1-\frac{1}{2^{\ell}-1}\right)}$

例：多重度$\ell=3$、ハッシュ値の総数Nが2000bit値の場合、
既存手法の計算時間に比べ、提案手法の計算時間は１０億倍程度高速
N:2000bit値➡ $N^{\frac{4}{9}}:N^{\frac{3}{7}}\approx 1,000,000,000:1$

動作の概略（ 3-衝突発見問題を例に）

1. 部分集合$I\subset[N]$をサンプルし、Iの像$f(I)$を計算($[N]\equiv\{1,\cdots,N\}$)
2. Iの要素と2-衝突を構成する部分集合$J\subset[N]\setminus I$ を探索し、像$f(J)$を計算
3. IおよびJ の要素と3-衝突を構成する要素$k\in[N]\setminus(I\cup J)$を探索
4. 得られた3-衝突の３つ組み (i,j,k) を出力

1.部分集合Iをサンプル
2. $J\subset[N]\setminus I$ を量子的に探索
3. $k\in[N]\setminus(I\cup J)$ を量子的に探索



関連文献

[1] A. Hosoyamada, Y. Sasaki, S. Tani, K. Xagawa, “Improved quantum multicollision-finding algorithm,” in *Proc. 10th International Conference on Post-Quantum Cryptography (PQCrypto 2019)*, pp. 350–367, vol. 11505, 2019.
[2] A. Hosoyamada, Y. Sasaki, S. Tani, K. Xagawa, “Quantum algorithm for the multicollision problem,” *Theoretical Computer Science*, vol. 842, pp. 100–117, 2020.

連絡先

谷 誠一郎（Seiichiro Tani）メディア情報研究部 情報基礎理論研究グループ
Email: cs-openhouse-ml@hco.ntt.co.jp